METHODS FOR COMPUTING THE CRC OF A MESSAGE FROM THE INCREMENTAL CRCs OF COMPOSITE SUB-MESSAGES

Vicente V. Cavanna & Patricia A. Thaler

ABSTRACT

Methods for adjusting an m-bit CRC of sub-messages are provided. Such adjustments enable the computation of the CRC of a message by XORing the partial or incremental CRCs of composite sub-messages corresponding to the sub-messages. In a first method, the contents of an m-bit memory location are field squared and stepped to the next state as determined by the Galois field generated by the CRC generating polynomial to adjust the m-bit CRC. In a second method, the partial m-bit CRC of a sub-message is calculated according to CRC generating polynomial, P(x). A variable Y is calculated using a lookup table, where $Y = x^n$ modulo P(x). The partial m-bit CRC and Y are multiplied together and divided by P(x). The remainder of the division forms the adjusted m-bit CRC.